

## UNITED STATES DISTRICT COURT

for the  
Western District of Washington

In the Matter of the Search of  
*(Briefly describe the property to be searched  
 or identify the person by name and address)*  
 Information associated with Snapchat Account  
 bbspokane that is stored at premises owned,  
 maintained, controlled, or operated by Snap, Inc.

Case No. MJ24-347

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:  
 Information associated with Snapchat Account bbspokane that is stored at premises owned, maintained, controlled, or operated by Snap, Inc.

located in the Southern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section*  
 18 U.S.C. § 2252(a)(2),(b)(2)

*Offense Description*  
 Possession of Child Pornography

The application is based on these facts:

- ☒ See Affidavit of Special Agent Sara K. Blond, continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.



*Applicant's signature*

Sara K. Blond, Special Agent (FBI)  
*Printed name and title*

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or  
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 06/07/2024



*Judge's signature*

City and state: Seattle, Washington

Paula L. McCandlis, United States Magistrate Judge  
*Printed name and title*

1                                   **AFFIDAVIT OF SPECIAL AGENT SARA BLOND**

2 STATE OF WASHINGTON        )

3                                   )       ss

4 COUNTY OF KING            )

5  
6           I, Sara Blond, a Special Agent with the Federal Bureau of Investigation (FBI),  
7 Seattle, Washington, having been duly sworn, state as follows:

8                                   **AFFIANT BACKGROUND**

9           1.       I am a Special Agent (“SA”) with the Federal Bureau of Investigation  
10 (“FBI”) and have been so employed since 2009. I am a law enforcement officer of the  
11 United States, within the meaning of Title 18, United States Code, who is empowered by  
12 law to conduct investigations of, and to make arrests for offenses enumerated in Title 18,  
13 United States Code.

14          2.       I am assigned to the Everett and Bellingham Resident Agencies of the  
15 FBI’s Seattle Field Office, where I specialize in Violent Crimes Against Children and  
16 Human Trafficking investigations occurring in Snohomish, Skagit, Whatcom, Island, and  
17 San Juan counties, which are situated in the Western District of Washington. I am  
18 assigned to the FBI Seattle’s Crimes Against Children & Human Trafficking Task Force,  
19 which includes investigations of the online sexual exploitation of children involving the  
20 transmission, possession and production of child pornography, exploitation of children on  
21 the internet, and other federal criminal activity. I am also a member of the Seattle  
22 Internet Crimes Against Children Task Force (“Seattle ICAC”). The goal of the Seattle  
23 ICAC is to catch distributors of child sexual abuse material (CSAM) on the Internet,  
24 whether delivered on-line or solicited on-line and distributed through other channels and  
25 to catch sexual predators who solicit victims on the Internet through chat rooms, forums  
26 and other methods.

3. During my career as an FBI Special Agent, I have served as the case agent in numerous child exploitation investigations. I have participated in all aspects of child exploitation investigations, including conducting surveillance, undercover operations, identifying victims, interviewing suspects, and executing arrest and search warrants. In 2015, I underwent specialized training facilitated by the FBI. I successfully completed coursework to become a Digital Evidence Extraction Technician, as authorized by the FBI's Computer Analysis and Response Team. In this capacity, I have specialized training in computer forensics, which involves the search, seizure, and extraction of digital evidence; this requires on-going mandatory training on an annual or semi-annual basis. I have worked as the case agent on numerous investigations involving child pornography, serving as the affiant on search warrants, complaints, and arrest warrants.

4. The information contained in this affidavit consists of my personal knowledge gained through this investigation, information provided by other law enforcement officers involved in this investigation, information provided by witnesses and others with knowledge of the relevant events and circumstances, information gleaned from my review of evidence, and my training and experience. Because this affidavit is offered for the limited purpose of establishing probable cause, I list only those facts that I believe are necessary to support such a finding. I do not purport to list every fact known to me or others as a result of this investigation.

#### **PURPOSE OF AFFIDAVIT**

5. I make this affidavit in support of an application for a search warrant for information associated with a certain Snapchat account that is stored at premises owned, maintained, controlled, or operated by Snap, Inc. ("Snapchat"), a company headquartered in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require

1 Snapchat to disclose to the government records and other information in its possession,  
2 pertaining to the subscriber or customer associated with the account.

3 6. Based on my training and experience and the facts as set forth in this  
4 affidavit, there is probable cause to believe that violations of Title 18 United States Code  
5 Section 2252(a)(4)(B), Possession of Child Pornography have been committed by  
6 JEREMY DAVID BRINKMAN. There is also probable cause to search the information  
7 described in Attachment A for evidence of these crimes and contraband or fruits of these  
8 crimes, as described in Attachment B.

9 **DEFINITIONS**

10 The following definitions apply to this affidavit:

11 7. “Chat,” as used herein, refers to any kind of text communication over the  
12 internet that is transmitted in real-time from sender to receiver. Chat messages are  
13 generally short in order to enable other participants to respond quickly and in a format  
14 that resembles an oral conversation. This feature distinguishes chatting from other text-  
15 based online communications such as internet forums and email.

16 8. For the purposes of this affidavit, a “minor” refers to any person less than  
17 eighteen years of age and for the purpose of this search warrant, “Child pornography,” as  
18 used herein, is defined in 18 U.S.C. § 2256 (any visual depiction of sexually explicit  
19 conduct where (a) the production of the visual depiction involved the use of a minor  
20 engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer  
21 image, or computer-generated image that is, or is indistinguishable from, that of a minor  
22 engaged in sexually explicit conduct, or (c) the visual depiction has been created,  
23 adapted, or modified to appear that an identifiable minor is engaged in sexually explicit  
24 conduct).

25 9. “Sexually explicit conduct” means actual or simulated (a) sexual  
26 intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons  
27

1 of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic  
2 abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18  
3 U.S.C. § 2256(2).

4 10. “Cloud-based storage service,” as used herein, refers to a publicly  
5 accessible, online storage provider that collectors of depictions of minors engaged in  
6 sexually explicit conduct can use to store and trade depictions of minors engaged in  
7 sexually explicit conduct in larger volumes. Users of such a service can share links and  
8 associated passwords to their stored files with other traders or collectors of depictions of  
9 minors engaged in sexually explicit conduct in order to grant access to their collections.  
10 Such services allow individuals to easily access these files through a wide variety of  
11 electronic devices such as desktop and laptop computers, mobile phones, and tablets,  
12 anywhere and at any time. An individual with the password to a file stored on a cloud-  
13 based service does not need to be a user of the service to access the file. Access is free  
14 and readily available to anyone who has an internet connection.

15 11. “Computer,” as used herein, refers to “an electronic, magnetic, optical,  
16 electrochemical, or other high speed data processing device performing logical or storage  
17 functions, and includes any data storage facility or communications facility directly  
18 related to or operating in conjunction with such device,” including smartphones and  
19 mobile devices.

20 12. “Data,” as used herein refers to the quantities, characters, or symbols on  
21 which operations are performed by a computer, being stored and transmitted in the form  
22 of electrical signals and recorded on magnetic, optical, or mechanical recording media.

23 13. “Digital Devices” as used herein refers to any physical object that has a  
24 computer, microcomputer, or hardware that is capable of receiving, storing, possessing,  
25 or potentially sending data.

26 14. “File Transfer Protocol” (“FTP”), as used herein, is a standard network  
27 protocol used to transfer computer files from one host to another over a computer

1 network, such as the internet. FTP is built on client-server architecture and uses separate  
2 control and data connections between the client and the server.

3 15. "Internet Service Providers" ("ISPs"), as used herein, are commercial  
4 organizations, community-owned, non-profit, or otherwise privately-owned companies  
5 that are in business to provide individuals and businesses access to the internet. ISPs  
6 provide a range of functions for their customers including access to the internet, web  
7 hosting, e-mail, remote storage, and co-location of computers and other communications  
8 equipment.

9 16. "Mobile applications," as used herein, are small, specialized programs  
10 downloaded onto mobile devices that enable users to perform a variety of functions,  
11 including engaging in online chat, reading a book, or playing a game.

12 17. "Records," "documents," and "materials," as used herein, include all  
13 information recorded in any form, visual or aural, and by any means, whether in  
14 handmade, photographic, mechanical, electrical, electronic, or magnetic form.

15 18. "User Attributes," as used herein refers to any tangible data, documents,  
16 settings, programs, or other information that provides information related to the identity  
17 of the specific user of the device, computer, application, program, or record.

### 18 **BACKGROUND**

19 19. Based on my training, experience and collaboration with agents/detectives  
20 investigation child exploitation, industry experts, academia and other law enforcement  
21 personnel, I know the below detailed information.

22 20. That adult persons with a sexual interest in minors are persons whose  
23 sexual targets are children. They receive sexual gratification and satisfaction from actual  
24 physical contact with children, fantasy involving the use of writings detailing physical  
25 contact with children, and/or from fantasy involving the use of pictures and/or videos of  
26 minors.  
27



1           21.     The development of the computer has changed the way children are  
2 engaged in sexually explicit conduct and the files created therefrom are distributed  
3 thereafter. The computer serves four functions in connection with depictions of children  
4 engaged in sexually explicit conduct. These four functions include: production,  
5 communications, distribution, and storage.

6           22.     Pornographers produce both still and moving images, i.e.: photographs and  
7 video. These files can be transferred either directly from the camera/camera phone into a  
8 computer or mobile application, directly from a storage device such as a flash drive to a  
9 computer, or the image files can be transferred directly into the computer by use of a  
10 scanner.

11           23.     In addition to data sharing between phones, mobile and desktop  
12 applications, and websites, e-mail may also be used electronically transmits files through  
13 a user's electronic device.

14           24.     All that a smart phone or computer user needs to do in order to use an  
15 application, website, or email is open up an account with one of the myriad of companies  
16 that provide services (e.g. Meta, Microsoft, Google, Discord, Snapchat, Dropbox, etc.).  
17 Once the account is set up, the user can choose the "name" of his/her account, which does  
18 not have to match (or even relate to) identifying information of the user. Thus, the user  
19 name by itself does nothing to identify the owner of the account, the user, or the  
20 composer of the communication. Nevertheless, often times the communications  
21 themselves, contain information that either directly or indirectly identifies the composer  
22 of the file. Based on my training and experience investigating child exploitation  
23 offenses, I know it is common for collectors of depictions of minors engaged in sexually  
24 explicit conduct to use multiple social media accounts and/or applications in order  
25 conceal their true identity and/or more easily categorize their collection according to the  
26 type of material or source.

1           25. Individuals involved in computer-related crimes often use these accounts to  
2 conduct both criminal and non-criminal communications. Consequently, these  
3 communications can be a great source of information to help identify the sender and/or  
4 recipient of the file and/or message. The ability to view these communications by  
5 investigating law enforcement often provides further investigative leads to assist in  
6 identifying the person of interest.

7           26. I know that an Internet Protocol (IP) address is a numerical label assigned  
8 to devices communicating on the internet and that the Internet Assigned Numbers  
9 Authority (IANA) manages the IP address space allocations globally. An IP address  
10 provides the methodology for communication between devices on the internet. It is a  
11 number that uniquely identifies a device on a computer network and, using transport  
12 protocols, moves information on the internet. Every device directly connected to the  
13 internet must have a unique IP address.

14           27. An IP address is typically comprised of four (4) series of numbers separated  
15 by periods and is most commonly represented as a 32-bit number such as  
16 71.227.252.216 (Internet Protocol Version 4). IPv6 is deployed as well and is  
17 represented as a 128-bit number such as 2001:db8:0:1234:0:567:8:1.

18           28. IP addresses are owned by the Internet Service Provider and leased to a  
19 subscriber/customer for a period of time. They are public and visible to others as you  
20 surf the internet. The lessee has no expectation of privacy due to the public nature of IP  
21 addresses.

22           29. When an Internet Service Provider's customer logs onto the internet using a  
23 computer or another web-enabled device, they are assigned an Internet Protocol (IP)  
24 address.

25           30. There are two different types of Internet Protocol addresses. The first is a  
26 dynamic IP address, which means the user's IP address may change each time they log on  
27 to the internet. The frequency in which this address changes is generally controlled by



1 the Internet Service Provider and not the user. The other type of IP address is a static IP  
2 address, which means that a user is assigned a specific IP address that remains constant  
3 every time they log on to the internet.

4 31. IP addresses are similar to a license plate on a motor vehicle. They are the  
5 property of the issuer, and not the vehicle owner. Just as your license plate is visible as  
6 you cruise your city or town, your IP address is visible as you cruise the internet. Your  
7 IP address is visible to the administrators of websites you visit, attached emails you send,  
8 and broadcast during most internet file and information exchanges that occur on the  
9 internet.

10 32. I know based on my training and experience, that Electronic Service  
11 Providers (“ESP”) and/or Internet Service Providers (“ISP,” collectively ISP) typically  
12 monitor their services utilized by subscribers. To prevent their communication networks  
13 from serving as conduits for illicit activity and pursuant to the terms of user agreements,  
14 ISPs routinely and systematically attempt to identify suspected depictions of minors  
15 engaged in sexually explicit conduct that may be sent through its facilities. Commonly,  
16 customer complaints alert them that an image or video file being transmitted through  
17 their facilities likely contains suspected depictions of minors engaged in sexually explicit  
18 conduct.

19 33. When an ESP/ISP receives such a complaint or other notice of suspected  
20 depictions of minors engaged in sexually explicit conduct, they may employ a “graphic  
21 review analyst” or an equivalent employee to open and look at the image or video file to  
22 form an opinion as to whether what is depicted likely meets the federal criminal  
23 definition of depictions of minors engaged in sexually explicit conduct found in 18 USC  
24 § 2256, which is defined as any visual depiction, including any photograph, film, video,  
25 picture, or computer or computer-generated image or picture, whether made or produced  
26 by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the  
27 production of such visual depiction involves the use of a minor engaging in sexually

1 explicit conduct; (B) such visual depiction is a digital image, computer image, or  
2 computer-generated image that is, or is indistinguishable from, that of a minor engaging  
3 in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or  
4 modified to appear that an identifiable minor is engaging in sexually explicit conduct. If  
5 the employee concludes that the file contains what appears to be depictions of minors  
6 engaged in sexually explicit conduct, a hash value of the file can be generated by  
7 operation of a mathematical algorithm. A hash value is an alphanumeric sequence that is  
8 unique to a specific digital file. Any identical copy of the file will have exactly the same  
9 hash value as the original, but any alteration of the file, including even a change of one or  
10 two pixels, results in a different hash value. Consequently, an unknown image can be  
11 determined to be identical to an original file if it has the same hash value as the original.  
12 The hash value is, in essence, the unique fingerprint of that file, and when a match of the  
13 “fingerprint” occurs, the file also matches. Several different algorithms are commonly  
14 used to hash-identify files, including Message Digest 5 (MD5) and Secure Hash  
15 Algorithm 1 (SHA-1).

16 34. Hash values are a very reliable method of authenticating files. It can be  
17 concluded with an extremely high degree of certainty that two files sharing the same hash  
18 value also share identical content. Based on my training and experience, as well as others  
19 in this field, I know it is more likely that two humans would share the same biological  
20 DNA than for two files to share the same hash value. If even one bit (the smallest  
21 measure of data in a file) of a file is changed, the entire hash value of that file changes  
22 completely. As an example that demonstrates the uniqueness of a SHA-1 hash, the  
23 likelihood of two files having the same SHA-1 hash value is  $2^{128}$  or:1 in  
24 340,000,000,000,000,000,000,000,000,000,000,000,000,000,000 chance. In an August 6<sup>th</sup>, 2020  
25 article in Live Science<sup>1</sup>, according to Professor Simona Francese, PhD, a forensic

26  
27 <sup>1</sup> Baker, Harry. “Do Identical Twins Have Identical Fingerprints?” LiveScience, Purch, 7 Aug. 2021,  
<https://www.livescience.com/do-identical-twins-have-identical-fingerprints.html>.

1 scientist and fingerprint expert from Sheffield Hallam University in the United Kingdom,  
 2 the likelihood of two humans having the same fingerprint is estimated to be:1 in  
 3 64,000,000,000.<sup>2</sup>

4 35. For two different files to have the same hash value is called a *collision*. I  
 5 know from experience that there have been no documented incidents of a collision  
 6 involving SHA-1 hash values “in the wild” since its creation in 1995. I am, however,  
 7 aware of a reported collision involving two files sharing the same SHA-1 value in a lab  
 8 setting. This was done purposely by engineers at Google<sup>3</sup> in 2017 under controlled  
 9 conditions for the sole purpose of creating this collision. Even with this knowledge in  
 10 mind, I am confident that the possibility of a suspected child sexual abuse material file  
 11 reported in a CyberTip having the same hash value as an unrelated, non-criminal file is  
 12 extremely unlikely. I believe hash value comparison is a highly reliable method of  
 13 determining if two files are the same or different, and that a confirmed hash match  
 14 between two files is a forensic finding on a par with a DNA match or a fingerprint match.

15 36. ESPs typically maintain a database of hash values of files that they have  
 16 determined to meet the federal definition of depictions of minors engaged in sexually  
 17 explicit conduct found in 18 USC § 2256. The ISPs typically do not maintain the actual  
 18 suspect files themselves; once a file is determined to contain suspected depictions of  
 19 minors engaged in sexually explicit conduct, the file is deleted from their system.

20 37. The ESPs can then use Image Detection and Filtering Process (“IDFP”),  
 21 Photo DNA (pDNA), or a similar technology which compares the hash values of files  
 22 embedded in or attached to transmitted files against their database containing what is  
 23  
 24

---

25 <sup>2</sup> Of note, in the same article, Professor Francese, who is a peer-reviewed, published scientist, commented, “to this  
 26 day, no two fingerprints have been found to be identical.”

27 <sup>3</sup> “Announcing the First sha1 Collision.” *Google Online Security Blog*, 23 Feb. 2017,  
<https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html>.

1 essentially a catalog of hash values of files that have previously been identified as  
2 containing suspected depictions of minors engaged in sexually explicit conduct.

3 38. When the ESP detects a file passing through its network that has the same  
4 hash value as an image or video file of suspected depictions of minors engaged in  
5 sexually explicit conduct contained in the database through a variety of methods, the ISP  
6 reports that fact to National Center for Missing and Exploited Children (NCMEC) via the  
7 latter's CyberTipline. By statute, an ESP or ISP has a duty to report to NCMEC any  
8 apparent depictions of minors engaged in sexually explicit conduct it discovers "as soon  
9 as reasonably possible." 18 U.S.C. § 2258A(a)(1). The CyberTip line report transmits  
10 the intercepted file to NCMEC. Often that occurs without an ISP employee opening or  
11 viewing the file because the files hash value, or "fingerprint," has already been associated  
12 to a file of suspected depictions of minors engaged in sexually explicit conduct. The  
13 ISP's decision to report a file to NCMEC is made solely on the basis of the match of the  
14 unique hash value of the suspected depictions of minors engaged in sexually explicit  
15 conduct to the identical hash value in the suspect transmission.

16 39. ESP's also monitor which devices are used to access their platform by  
17 recording the advertising identification number. This number is a unique identifier  
18 assigned to hardware devices used by ESP's to track users semi-anonymously and  
19 provide targeted advertisements. Because it is a unique identifier, this information can  
20 link specific devices owned by specific individuals with the criminal activity on a  
21 particular platform's account.

22 40. Most Internet Service Providers keep subscriber records relating to the IP  
23 address they assign, and that information is available to investigators. Typically, an  
24 investigator has to submit legal process (e.g. subpoena or search warrant) requesting the  
25 subscriber information relating to a particular IP address at a specific date and time.

26 41. A variety of publicly available websites provide a public query/response  
27 protocol that is widely used for querying databases in order to determine the registrant or

1 assignee of internet resources, such as a domain name or an IP address block. These  
2 include WHOIS, MaxMind, arin.net, and other common search tools.

3 42. The act of “downloading” is commonly described in computer networks as  
4 a means to receive data to a local system from a remote system, or to initiate such a data  
5 transfer. Examples of a remote system from which a download might be performed  
6 include a webserver, FTP server, email server, or other similar systems. A download can  
7 mean either any file that is offered for downloading or that has been downloaded, or the  
8 process of receiving such a file. The inverse operation, “uploading,” refers to the sending  
9 of data from a local system to a remote system such as a server or another client with the  
10 intent that the remote system should store a copy of the data being transferred, or the  
11 initiation of such a process.

12 43. The National Center for Missing and Exploited Children (NCMEC) is a  
13 private, non-profit organization established in 1984 by the United States Congress.  
14 Primarily funded by the Justice Department, the NCMEC acts as an information  
15 clearinghouse and resource for parents, children, law enforcement agencies, schools, and  
16 communities to assist in locating missing children and to raise public awareness about  
17 ways to prevent child abduction, child sexual abuse and depictions of minors engaged in  
18 sexually explicit conduct.

19 44. The Center provides information to help locate children reported missing  
20 (by parental abduction, child abduction, or running away from home) and to assist  
21 physically and sexually abused children. In this resource capacity, the NCMEC  
22 distributes photographs of missing children and accepts tips and information from the  
23 public. It also coordinates these activities with numerous state and federal law  
24 enforcement agencies.

25 45. The CyberTipline offers a means of reporting incidents of child sexual  
26 exploitation including the possession, manufacture, and/or distribution of depictions of  
27 minors engaged in sexually explicit conduct; online enticement; child prostitution; child

1 sex tourism; extra familial child sexual molestation; unsolicited obscene material sent to a  
2 child; and misleading domain names, words, or digital images.

3 46. Any incidents reported to the CyberTipline online or by telephone go  
4 through this three-step process: CyberTipline operators review and prioritize each lead;  
5 NCMEC's Exploited Children Division analyzes tips and conducts additional research;  
6 The information is accessible to the FBI, ICE, and the USFIS via a secure Web  
7 connection. Information is also forwarded to the ICACs and pertinent international, state,  
8 and local authorities and, when appropriate, to the ESP.

9 **INDIVIDUALS WITH A SEXUAL INTEREST IN MINORS**

10 47. Based upon my knowledge, experience, and training in depictions of  
11 minors engaged in sexually explicit conduct investigations, and the training and  
12 experience of other law enforcement officers with whom I have had discussions, I know  
13 that there are certain characteristics common to individuals with a sexual interest in  
14 minors who are involved in depictions of minors engaged in sexually explicit conduct as  
15 described below.

16 48. Those who possess, receive and attempt to receive depictions of minors  
17 engaged in sexually explicit conduct may receive sexual gratification, stimulation, and  
18 satisfaction from contact with children; or from fantasies they may have viewing children  
19 engaged in sexual activity or in sexually suggestive poses, such as in person, in  
20 photographs, or other visual media; or from literature describing such activity. As  
21 described in detail below, BRINKMAN utilized Snapchat and Kik to receive and  
22 distribute child pornography files. Based upon BRINKMAN's 2007 conviction for  
23 Dealing in Depictions of Minors Engaged in Sexually Explicit Conduct coupled with his  
24 current federal prosecution for Possession of Child Pornography, there is ample evidence  
25 to confirm BRINKMAN's sexualized interest in minors.

26 49. Those who possess, receive and attempt to receive depictions of minors  
27 engaged in sexually explicit conduct may keep records, to include names, contact



1 information, and/or dates of their interaction, of the children they have attempted to  
2 seduce, arouse, or with whom they have engaged in the desired sexual acts.

3 50. Those who possess, receive, and attempt to receive depictions of minors  
4 engaged in sexually explicit conduct often maintain their collections that are in a digital  
5 or electronic format in a safe, secure, and private environment, such as a computer and  
6 surrounding area. These collections are often maintained for several years and are kept  
7 close by, usually at the individual's residence, to enable the collector to view the  
8 collection, which is valued highly. Again, BRINKMAN is a convicted sex offender who  
9 has maintained a sexualized interest in minors which he has cultivated by receiving and  
10 distributing depictions of minors engaged in sexually explicit conduct and by  
11 communicating with suspected minors in an effort to entice the production of child  
12 pornography files.

13 51. Those who possess, receive and attempt to receive depictions of minors  
14 engaged in sexually explicit conduct also may correspond with and/or meet others to  
15 share information and materials; rarely destroy correspondence from other depictions of  
16 minors engaged in sexually explicit conduct distributors/collectors; conceal such  
17 correspondence as they do their sexually explicit material; and often maintain lists of  
18 names, addresses, and telephone numbers of individuals with whom they have been in  
19 contact and who share the same interests in depictions of minors engaged in sexually  
20 explicit conduct.

21 52. Those who possess, receive, and attempt to receive depictions of minors  
22 engaged in sexually explicit conduct prefer not to be without their depictions of minors  
23 engaged in sexually explicit conduct for any prolonged time period. This behavior has  
24 been documented by law enforcement officers involved in the investigation of depictions  
25 of minors engaged in sexually explicit conduct throughout the world. The fact that  
26 BRINKMAN was arrested in 2006 for his collection of child sexual abuse material and  
27

continued through May 2024 to engage in the exact conduct serves as confirmation of his inability to be without child pornography for any prolonged period of time.

**BACKGROUND CONCERNING SNAP INC. (Snapchat)<sup>4</sup>**

53. Snapchat is a popular social media platform used for posting short videos, photos, memes, text messages and other electronic content. Like Facebook, Instagram, and other social media sites, posted content can be shared with your “friends” on the platform. The user has the option to share posts and/or communicate with their friends individually or with their entire friend group through “My Story.” Public posts made on “My Story” can be viewed for 24 hours before they disappear.

54. In my professional experience, having talked to other detectives that have investigated cases involving the use of Snapchat and have received historical data from previously written Snapchat warrants, I know that data stored in Snapchat user accounts, to include photos, videos, memes, instant message exchanges, geolocation data, and user information, provides valuable supporting evidence in criminal investigations.

55. Service Provider Identity: I have confirmed that the service provider receives and processes legal requests at: Snap Inc., ATTN: Custodian of Records, 2772 Donald Douglas Loop North, Santa Monica, CA 90405, lawenforcement@snapchat.com.

56. Service Provider Records: Subscriber information (often known as “registration information” for Internet applications or service) is obtained by the service provider when an account is established and typically includes information such as: The subscriber name, address, billing/payment information; account initiation date; changes to the account; type of account; custom account features; additional phone numbers, email addresses, and/or other contact information; additional persons having authority on the account; any additional accounts linked to the subject account; and unique identifiers

---

<sup>4</sup> The information in this section is based on information published by Snapchat's “Privacy Policy” website, including, but not limited to, the following webpages: “Privacy Policy available at <https://values.snap.com/privacy/privacy-policy>, as well as the Snapchat Law Enforcement Guide.

1 for the device using the target address, and other devices the customer of the subject  
 2 account uses. In my experience, this information frequently provides investigative leads.

3 57. The following is an excerpt from Snapchat's website discussing the types  
 4 of information they collect:

5 *Information We Get When You Use Our Services*

6 *When you use our services, we collect information about which of those services*  
 7 *you've used and how you've used them. We might know, for instance, that you*  
 8 *watched a particular Story, saw a specific ad for a certain period of time, and sent*  
 9 *a few Snaps. Here's a fuller explanation of the types of information we collect*  
 10 *when you use our services:*

11 *Usage Information. We collect information about your activity through our*  
 12 *services. For example, we may collect information about:*

- 13 • *how you interact with our services, such as which filters you view or*  
 14 *apply to Snaps, which Stories you watch on Discover, whether*  
 15 *you're using Spectacles, or which search queries you submit.*
- 16 • *how you communicate with other Snapchatters, such as their names,*  
 17 *the time and date of your communications, the number of messages*  
 18 *you exchange with your friends, which friends you exchange*  
 19 *messages with the most, and your interactions with messages (such*  
 20 *as when you open a message or capture a screenshot).*
- 21 • *Content Information. We collect content you create on our services,*  
 22 *such as custom stickers, and information about the content you*  
 23 *create or provide, such as if the recipient has viewed the content and*  
 24 *the metadata that is provided with the content.*
- 25 • *Device Information. We collect information from and about the*  
 26 *devices you use. For example, we collect:*

- *information about your hardware and software, such as the hardware model, operating system version, device memory, advertising identifiers, unique application identifiers, apps installed, unique device identifiers, browser type, language, battery level, and time zone;*
- *information from device sensors, such as accelerometers, gyroscopes, compasses, microphones, and whether you have headphones connected; and*
- *information about your wireless and mobile network connections, such as mobile phone number, service provider, IP address, and signal strength.*
- *Device Phonebook. Because Snapchat is all about communicating with friends, we may—with your permission—collect information from your device’s phonebook.*
- *Camera and Photos. Many of our services require us to collect images and other information from your device’s camera and photos. For example, you won’t be able to send Snaps or upload photos from your camera roll unless we can access your camera or photos.*

*Location Information. When you use our services we may collect information about your location. With your permission, we may also collect information about your precise location using methods that include GPS, wireless networks, cell towers, Wi-Fi access points, and other sensors, such as gyroscopes, accelerometers, and compasses.*

*Information Collected by Cookies and Other Technologies. Like most online services and mobile applications, we may use cookies and other technologies, such as web beacons, web storage, and unique advertising*

1        *identifiers, to collect information about your activity, browser, and device.*  
 2        *We may also use these technologies to collect information when you*  
 3        *interact with services we offer through one of our partners, such as*  
 4        *advertising and commerce features. For example, we may use information*  
 5        *collected on other websites to show you more relevant ads. Most web*  
 6        *browsers are set to accept cookies by default. If you prefer, you can usually*  
 7        *remove or reject browser cookies through the settings on your browser or*  
 8        *device. Keep in mind, though, that removing or rejecting cookies could*  
 9        *affect the availability and functionality of our services. To learn more about*  
 10       *how we and our partners use cookies on our services and your choices,*  
 11       *please check out our Cookie Policy.*

12       *Log Information. We also collect log information when you use our*  
 13       *website, such as:*

- 14       • *details about how you've used our services;*
- 15       • *device information, such as your web browser type and language;*
- 16       • *access times;*
- 17       • *pages viewed;*
- 18       • *IP address;*
- 19       • *identifiers associated with cookies or other technologies that may*  
 20       *uniquely identify your device or browser; and*
- 21       • *pages you visited before or after navigating to our website.*
- 22       • *Information We Collect from Third Parties*

23       *We may collect information about you from other users, our affiliates, and third*  
 24       *parties. Here are a few examples:*

- 25       • *If you link your Snapchat account to another service (like Bitmoji or a*  
 26       *third-party app), we may receive information from the other service, like*  
 27       *how you use that service.*

- *Advertisers, app developers, publishers, and other third parties may share information with us as well. We may use this information, among other ways, to help target or measure the performance of ads. You can learn more about our use of this kind of third-party data in our Support Center.*
- *If another user uploads their contact list, we may combine information from that user's contact list with other information we have collected about you.*

### **SUMMARY OF PROBABLE CAUSE**

58. In mid-March of 2024, I was contacted Det. Andrew McLauchlan, Everett Police Department (EPD), regarding EPD's investigation into JEREMY DAVID BRINKMAN. Det. McLauchlan, who I know to be a fellow member of the Seattle ICAC, explained he had evidence of Brinkman trading child sexual abuse material (CSAM), which was derived from Cybertips. Det. McLauchlan said BRINKMAN had a prior felony conviction for CSAM-related offenses; BRINKMAN was relieved of his duty to register as a sex offender in 2019. Det. McLauchlan said that in reviewing some of BRINKMAN's online chats, BRINKMAN claimed he was having sex with a 12-year-old girl in his neighborhood.

59. Over the following weeks, I met with Det. McLauchlan to discuss the case and review the related CSAM. Det. McLauchlan sent me the Cybertips from the National Center for Missing and Exploited Children (NCMEC) related to BRINKMAN, which I reviewed.

60. Based on my training and experience, I know that Electronic Service Providers ("ESPs") (e.g. Google, Meta, Snapchat, Yahoo) typically monitor their own services used by their subscribers. To prevent their communication networks from serving as conduits for illicit activity and pursuant to the terms of user agreements, ESPs routinely and systematically attempt to identify suspected depictions of minors engaged in sexually explicit conduct that may be sent through their facilities. For example, an ESP may check the unique value, which is series of numbers known as a SHA-1 hash



1 value, of a subscriber's uploaded photos to see if it has been previously identified as  
2 CSAM.

3 61. When the ESP detects a file passing through its network that has the same  
4 hash value as an image or video file of suspected depictions of minors engaged in  
5 sexually explicit conduct contained in the database through a variety of methods, the ESP  
6 reports that fact to NCMEC's CyberTipline. By statute, an ESP has a duty to report to  
7 NCMEC any apparent depictions of minors engaged in sexually explicit conduct it  
8 discovers "as soon as reasonably possible." 18 U.S.C. § 2258A(a)(1). The CyberTipline  
9 report transmits the intercepted file from the ESP to NCMEC. Often that occurs without  
10 an ESP employee opening or viewing the file because the files hash value, which acts like  
11 the file's "fingerprint," has already been associated to a file of suspected depictions of  
12 minors engaged in sexually explicit conduct. The ESP's decision to report a file to  
13 NCMEC is made solely on the basis of the match of the unique hash value of the  
14 suspected depictions of minors engaged in sexually explicit conduct to the identical hash  
15 value in the suspect transmission.

16 62. In a Cybertip from Meet Me, which is a dating website, from December of  
17 2023, a user with the display name "aaa" and email address of  
18 jeremy.d.brinkman@gmail.com was chatting with a female user about child rape. The  
19 conversation between the user and the woman are flirtations in nature. Specifically, the  
20 user, later identified as BRINKMAN, told the woman about repeated sexual encounters  
21 he had with another person. When the woman asks BRINKMAN if he had sex recently,  
22 BRINKMAN responded, "I've been fucking that cutie I showed you last time" adding  
23 "she can't come over too often but we got to fuck for about an hour on Friday night."  
24 BRINKMAN then described the various sex acts he performed on that female, saying  
25 "shes so tiny and tight and she can't suck too much of my cock yet." BRINKMAN  
26 instructed the woman to guess the age of the other person he'd repeatedly slept with.  
27 When the woman didn't guess, BRINKMAN said, "Ah shes just 12 really." In reference

1 to the 12-year-old child, BRINKMAN goes on to say, “She lives just in the next  
2 apartment building too so she’s really close.”

3 63. In another Cybertip from Kik, which is a mobile messaging app, from  
4 October of 2023, a user with the username “reddyredhead69\_32i” and the email address  
5 of jeremy.d.brinkman@gmail.com was reported to NCMEC for sharing CSAM with  
6 another user. Kik reviewed three CSAM files shared by the user, later identified as  
7 BRINKMAN, which they sent to NCMEC. One of the three CSAM files Kik sent to  
8 NCMEC was reviewed by NCMEC, then flagged as CSAM with the categorization of a  
9 pubescent minor engaged in lascivious exhibition of the genitals.

10 64. Suspecting the email address in both Cybertips reflected the user’s true  
11 name, Det. McLauchlan searched law enforcement databases for “Jeremy Brinkman.”  
12 This returned one person, BRINKMAN, who resided at XXXX Chestnut St, Apartment  
13 X, Everett, Washington. Det. McLauchlan reviewed BRINKMAN’s criminal history,  
14 which showed a 2007 conviction for Dealing in Depictions of Minors Engaged in  
15 Sexually Explicit Conduct. Similarly, Det. McLauchlan noticed the driver’s license  
16 photo for BRINKMAN was visually similar to the dating profile photo from the Meet Me  
17 user.

18 65. The IP address in both Cybertips was the same, and it resolved to Comcast  
19 Cable. A warrant to Comcast for this user’s subscriber information returned to Jeremy  
20 Brinkman, XXXX Chestnut St, Apartment X, Everett, Washington. A similar warrant to  
21 Google for jeremy.d.brinkman@gmail.com returned the user’s first name as Jeremy. The  
22 Google returns also listed the user’s year of birth as 1981. The same date of birth is listed  
23 the Meet Me Cybertip, and it is BRINKMAN’s actual date of birth.

24 66. On April 2, 2024, EPD served a search warrant to Kik on for content of  
25 reddyredhead69\_32i’s account. On or about April 30, 2024, I met with Det. McLauchlan  
26 to preview the CSAM from the Kik search warrant return. EPD later released a copy of  
27 the CSAM to FBI, which I reviewed. Based on my review of BRINKMAN’s Kik

account, I observed the following CSAM files which I believe meet the federal definition of child pornography as defined in 18 U.S.C. 2256(8):

a. Filename: 0d402947-503f-4ca7-882e-38ff2fd98d09.mp4 File type: Video Length: 49 seconds Description: This video depicts a young girl wearing a green t-shirt and no bottoms. The child is kneeling. An erect male penis is inserted into her mouth with a male's hand masturbating the penis while the child performs oral sex. At one point, the child opens her mouth to reveal a white, milky substance, which she swallows. Towards the end of the video, the child waves and smiles at the camera. There are white and purple bedsheets visible behind the child. Based on the size of the child's body relative to the size of the adult male, I estimate this child is between 5 and 8 years old.

b. Filename: 0f3dc5d8-1e86-4c7d-891d-a1e3869eda28.mp4 File type: Video Length: 1 minute and 30 seconds Description: This video depicts a young girl wearing a floral shirt and bunny rabbit plastic ring on her finger. The child is sitting on her knees, situated between the open legs of an adult female. The adult female is naked. The child's mouth is inserted into the vagina of the adult female. The adult female can be heard moaning. The angle of the camera is from the adult female's torso downward, suggesting the adult female is filming the child. Towards the end of the video, the camera angle changes and films a Christmas tree. A woman can be heard speaking a language other than English. Based on the size of the child relative to the adult's legs, including the size of her face and facial features, I estimate this child is between 4 and 8 years old.

c. Filename: 3fedae6f-7818-4d6b-ae38-086ea4f615a0.mp4 File type: Video Length: 27 seconds Description: This video depicts a young boy's nude genitals and torso. The child's erect penis is clearly visible, and it is situated across from an adult woman who is also nude. The woman's legs are spread, and she uses her fingers to spread her labia. The young boy repeatedly inserts his penis into the adult woman's vagina. The woman can be heard saying "good boy" and the child attempts and continues to penetrate her. Cartoon sounds can be heard in the background. The camera angle is angled down the woman's torso, suggesting she is filming the child. Based on the size of the child's penis and torso, particularly when compared against the size of the adult woman's legs and vagina, I estimate this child is between 2 and 5 years old.

67. The search warrant returns from Kik also contain several "selfie" type photos that were visually similar to BRINKMAN's driver's license photo.

68. On May 8, 2024, I accompanied EPD on a residential search warrant of Brinkman's home, located at XXXX Chestnut St, Apartment X, Everett, Washington. EPD located BRINKMAN just outside of his apartment, then arrested him. During the

1 execution of the search warrant, I walked through BRINKMAN's apartment and noticed  
2 a Samsung Galaxy S9 cell phone on the armrest of the couch. The lock screen displayed  
3 the text "Jeremy Brinkman." In a post-Miranda statement, BRINKMAN identified the  
4 Samsung Galaxy S9 cell phone as his cell phone.

5 69. In a post-Miranda interview with me and Det. McLauchlan, BRINKMAN  
6 admitted to using Kik and Snapchat, plus Meet Me and other dating sites, to connect with  
7 others online and trade CSAM. BRINKMAN described different ways he could get  
8 others to send him CSAM once he determined they were similarly "like-minded."

9 70. BRINKMAN specifically identified the Samsung Galaxy S9 cell phone as  
10 his primary means for accessing CSAM. BRINKMAN did not think investigators would  
11 find CSAM on other digital devices located in his home.

12 71. Regarding Snapchat, BRINKMAN said he used it briefly but never really  
13 got the hang of it. BRINKMAN said many of the individuals he met on dating sites often  
14 wanted to move their conversations with BRINKMAN onto Snapchat specifically.

15 72. BRINKMAN identified several email accounts of his, which included  
16 jeremy.d.brinkman@outlook.com and possibly also jeremy.d.brinkman@gmail.com.

17 73. BRINKMAN described looking at CSAM as a cathartic stress release for  
18 him. BRINKMAN said he struggled to control his addiction to CSAM for years, even  
19 after his prior conviction in 2007. BRINKMAN knew CSAM was exploitative of the  
20 children depicted in the images, which he knew was wrong. BRINKMAN said he would  
21 often delete CSAM files once his feelings of shame surrounding his CSAM possession  
22 became unbearable. BRINKMAN denied any hands-on offenses, stating any  
23 conversations he had about abusing children were fantasy. BRINKMAN similarly denied  
24 ever seeking out actual children online.

25 74. Following BRINKMAN's arrest by EPD, I was forwarded another  
26 Cybertip, which was filed by Snapchat for the account **bbspokane**. I read the Cybertip  
27 and noticed the subscriber information for **bbspokane** listed the user's phone number as

(425) 299-2088. I recognized this as a phone number associated with BRINKMAN. According to what Det. McLauchlan told me, BRINKMAN provided a witness statement to EPD in an unrelated investigation and listed that as his cell phone number. In summary, the Snapchat Cybertip indicated user **bbspokane** uploaded suspected CSAM into a chat message. I know Snapchat is predominantly used on mobile devices, such as the seized Samsung Galaxy S9 cell phone.

75. On May 22, 2024, I served a preservation request to Snapchat for username bbspokane. Snapchat's confirmation of receipt stated the account would be preserved for 90 days. Snapchat's also referenced the Cybertip they previously filed with NCMEC for **bbspokane**.

#### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

76. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Snapchat to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

#### **CONCLUSION**

77. Based on the information set forth herein, there is probable cause to search the above-described SUBJECT DIGITAL DEVICE, as further described in Attachment A, for evidence, fruits, and instrumentalities, of violations of Title 18 United States Code Sections 2252(a)(2),(b)(2) Possession of Child Pornography as further described in Attachment B.

78. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Snapchat. Because the warrant will be served on Snapchat,

1 who will then compile the requested records at a time convenient to it, reasonable cause  
2 exists to permit the execution of the requested warrant at any time in the day or night.

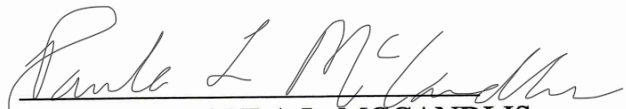
3 79. This Court has jurisdiction to issue the requested warrant because it is “a  
4 court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a),  
5 (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . .  
6 that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

7 80. The affidavit and application are being presented by reliable electronic  
8 means pursuant to Federal Rules of Criminal Procedure 4.1 and 41(d)(3).

9  
10 

11 SARA K. BLOND  
12 Special Agent  
13 Federal Bureau of Investigation  
14

15 The above-named agent provided a sworn statement attesting to the truth of the  
16 foregoing affidavit by telephone on this 7th day of June, 2024.

17 

18 THE HON. PAULA L. MCCANDLIS  
19 United States Magistrate Judge  
20  
21  
22  
23  
24  
25  
26  
27



**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with Snapchat Account **bbspokane** that is stored at premises owned, maintained, controlled, or operated by Snap, Inc, a company headquartered in Santa Monica, California.

**ATTACHMENT B****Particular Things to be Seized**

The following items, which constitute fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Section 2252(a)(4)(B) and (b)(2) Possession of Child Pornography, including:

**I. Information to be disclosed by Snapchat**

To the extent that the information described in Attachment **bbspokane** is within the possession, custody, or control of Snapchat, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Snapchat, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Snapchat is required to disclose the following information to the government for the user listed in Attachment A1 for the dates of August 17, 2019, (account creation date), to the date of compliance with this warrant/order:

a. Subscriber basic contact information including subscriber, name, birth date, email address(es), physical address (city, state, zip, country), all telephone numbers, screen name and any associated website;

b. Basic subscriber information (BSI) including Subscriber Identification Number, Date and Time stamp of account creation date displayed in GMT, IP address at account sign-up, Logs in GMT showing source and destination IP addresses and ports; most recent Logins in GMT, registered mobile number(s), verification on whether publicly viewable, and all advertising identification number(s), as well as all devices used to access the account, including IMEI numbers, ICCID numbers, and all descriptions of make and model, and push-tokens;

c. Customer service records: All subscriber contacts with customer support including notifications or complaints of the account being hacked or stolen, or any other issue with the use of or access to the Snapchat account that were created, uploaded, adjusted, accessed, used, modified, or deleted;

1 d. Subscriber financial account information and account status history;

2 e. Images: All photos, videos, and other depictions associated with the  
3 account, in any format or media. Law enforcement will search these files and only seize  
4 child pornography defined in 18 U.S.C. § 2256, in addition to all depictions which  
demonstrate dominion and control over the account;

5 f. Postings, communications, biographical information, or other  
6 information identifying the suspect account user and/or any other persons transmitting  
7 depictions of minors engaged in sexually explicit conduct or evidencing the transmissions  
thereof;

8 g. Usage information detailing how the suspect account interacted with  
9 Snapchat including filters used to apply to Snaps, which Stories the suspect account  
watched on Discover, whether the suspect account used Spectacles, or which search  
10 queries the suspect account user submit;

11 h. Usage information detailing how the suspect account communicated  
12 with other Snapchatters, such as their names, the time and date of your communications,  
the number of messages exchanged with other users, which other users exchanged  
13 messages with the suspect account, and the suspect account's interactions with messages  
(such as when the suspect account opened a message or captured a screenshot);

14 i. Content information including information about the content created  
15 or provided by the suspect account, such as if the recipient has viewed the content and the  
16 metadata that is provided with the content;

17 j. Device information documenting the devices used by the suspect  
18 account to include information about the suspect account's hardware and software (to  
include hardware model, operating system version, device memory, advertising  
19 identifiers, unique application identifiers, apps installed, unique device identifiers,  
browser type, language, battery level, and time zone);

20 k. Device information documenting device sensors, such as  
21 accelerometers, gyroscopes, compasses, microphones, and whether the suspect account  
22 has headphones connected;

23 l. Device information documenting the wireless and mobile network  
24 connections, to include mobile phone number, service provider, IP address, and signal  
strength;

25 m. Device information to include device Phonebook data collected, and  
26 any unique identifiers for devices used to access the account;

1           n.       Device information to include Camera and Photos collected from the  
suspect account's device's camera and photos;

2           o.       Location information about the suspect account's precise location  
3 using methods that include GPS, wireless networks, cell towers, Wi-Fi access points, and  
4 other sensors, such as gyroscopes, accelerometers, and compasses;

5           p.       Information collected by cookies and other technologies to include  
information when the suspect account interacted with services Snapchat offers through  
6 one of its partners, such as advertising and commerce features;

7           q.       Log information such as:

8                   i.       details about how the suspect account used Snapchat services;

9                   ii.      device information, such as the suspect account's web  
10 browser type and language;

11                  iii.     access times;

12                  iv.     pages viewed;

13                  v.      IP address;

14                  vi.     identifiers associated with cookies or other technologies that  
15 may uniquely identify the suspect account's device or browser; and

16                  vii.    pages the suspect account visited before or after navigating to  
17 Snapchat's website.

18           r.       Information collected from Third Parties about the suspect account  
19 from other users, Snapchat affiliates, and third parties to include if the suspect account  
20 linked it's Snapchat account to another service (like Bitmoji or a third-party app) or if  
another user uploads their contact list, Snapchat may combine information from that  
21 user's contact list with other information Snapchat have collected about the suspect  
22 account.

23           Snapchat is hereby ordered to disclose the above information to the government  
24 within **14 days** of issuance of this warrant.

25 //

26 //

1     **II. Information to be seized by the government**

2             All information described above in Section I that constitutes fruits, evidence and  
3 instrumentalities of violations of Title 18, United States Code, Section 2252(a)(4)(B) and  
4 (b)(2) Possession of Child Pornography since the creation of the account, including, for  
5 the user ID identified on Attachment A, information pertaining to the following matters:  
6

7             a. Evidence identifying the person(s) exercising dominion and control  
8 over the suspect account;

9             b. Financial account information and account status history;

10            c. Evidence indicating the targeting, communication, and solicitation of  
11 children to produce sexually explicit material, or the possession or distribution of such  
12 files;

13            d. All photos, videos, and other depictions associated with the account  
14 that depict child pornography defined in 18 U.S.C. § 2256;

15            e. Images associated with the account belonging to the Snapchat  
16 suspect account user;

17            f. Postings, communications, biographical information, or other  
18 information identifying the suspect account user and/or any other persons transmitting  
19 depictions of minors engaged in sexually explicit conduct or evidencing the transmissions  
20 thereof;

21            g. Usage information evidence and communications between  
22 **bbspokane** and others to include communications to target minors for sexual exploitation  
or to obtain child sexual abuse material (including when the suspect account opened a  
message or captured a screenshot);

23            h. Evidence of payment for receipt of child sexual abuse material;

24            i. Evidence indicating how and when the Snapchat account was  
25 accessed or used, to determine the chronological and geographic context of account  
26 access, use, and events relating to the crime under investigation and to the Snapchat  
27 account owner;

1 j. Information about the content created or provided by the suspect  
2 account, when the content was viewed and the metadata that is provided with the content;

3 k. Data related to linked services;

4 l. User attribution evidence identifying the account user's devices,  
5 software, sensors, operating version, advertising identifiers, installed applications, unique  
6 identifiers, browser data, time zone, wireless and mobile network connections to include  
7 numbers, providers, IP addresses, and data related thereto;

8 m. Evidence of the Snapchat account user's state of mind as it relates to  
9 the crimes under investigation;

10 n. The identity of the person(s) who created or used the user ID,  
11 including records that help reveal the whereabouts of such person(s), and to establish  
12 dominion and control over the account during this time period.

13 This warrant authorizes a review of electronically stored information, communications,  
14 other records and information disclosed pursuant to this warrant in order to locate  
15 evidence, fruits, and instrumentalities described in this warrant. The review of this  
16 electronic data may be conducted by any government personnel assisting in the  
17 investigation, who may include, in addition to law enforcement officers and agents,  
18 attorneys for the government, attorney support staff, and technical experts. Pursuant to  
19 this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the  
20 custody and control of attorneys for the government and their support staff for their  
21 independent review.  
22  
23  
24  
25  
26  
27